

Title (en)

Method for protecting an electronic circuit against fault-based attacks

Title (de)

Verfahren zur Sicherung von Schaltkreisen gegen fehlerbasierte Seitenkanalangriffe

Title (fr)

Procédé de sécurisation d'un ensemble électronique contre des attaques par introduction d'erreurs

Publication

**EP 1387519 A2 20040204 (FR)**

Application

**EP 02291728 A 20020709**

Priority

EP 02291728 A 20020709

Abstract (en)

The method involves performing an additional calculation by a verification function on an intermediate result to obtain a calculation signature. A part of the calculation is performed to recalculate the signature and compare them to detect a possible error. An elementary operation using another super-function operation is performed from a larger set. Independent claims are also included for the following: (a) an electronic assembly comprising storage unit of a calculation process (b) a computer program including program code instructions to execute the steps of securing an electronic assembly (c) a smart card comprising a storage unit of a calculation process.

Abstract (fr)

L'invention concerne un procédé de sécurisation d'un ensemble électronique mettant en oeuvre un algorithme quelconque contre les attaques par introduction d'erreur. Le procédé selon la présente invention consiste à effectuer un calcul supplémentaire par une fonction de vérification sur au moins un résultat intermédiaire afin d'obtenir une empreinte de calcul et à effectuer au moins une autre fois tout ou partie du calcul afin de recalculer ladite empreinte et de les comparer dans le but de détecter une éventuelle erreur. <IMAGE>

IPC 1-7

**H04L 9/06**

IPC 8 full level

**G06F 1/00** (2006.01); **G06F 7/38** (2006.01); **G06F 21/52** (2013.01); **H04L 9/06** (2006.01); **H04L 9/10** (2006.01)

CPC (source: EP US)

**G06F 7/38** (2013.01 - EP US); **G06F 21/52** (2013.01 - EP US); **G09C 1/00** (2013.01 - EP); **H04L 9/004** (2013.01 - EP US); **G06F 2207/7271** (2013.01 - EP US); **H04L 2209/127** (2013.01 - EP US)

Cited by

EP2166696B1

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR

DOCDB simple family (publication)

**EP 1387519 A2 20040204**; **EP 1387519 A3 20040218**; AU 2003249501 A1 20040123; AU 2003249501 A8 20040123; BR 0312561 A 20051220; EP 1552362 A2 20050713; JP 2005532728 A 20051027; JP 2011072040 A 20110407; JP 5401477 B2 20140129; US 2008130869 A1 20080605; US 7826610 B2 20101102; WO 2004006074 A2 20040115; WO 2004006074 A3 20040304

DOCDB simple family (application)

**EP 02291728 A 20020709**; AU 2003249501 A 20030707; BR 0312561 A 20030707; EP 03762843 A 20030707; IB 0303120 W 20030707; JP 2004519119 A 20030707; JP 2011002280 A 20110107; US 52080603 A 20030707